MARCH 2004

# virus BULLETIN

The International Publication on Computer Virus Prevention, Recognition and Removal

## CONTENTS



## IN THIS ISSUE

### ALL IN THE MIX

Take a little piece of W32/Mimail, a dash of social engineering, a pinch of W2K/Stream and share the code freely. Peter Ferrie describes the gaggle of variants that make up the Dumaru family.
**page 4**

### DOOM AND GLOOM

When a daily sports paper compares a national soccer crisis with the spread of an Internet worm, you know that the worm has had an enormous impact on everyday life. Gabor Szappanos tracks the rise of W32/Mydoom.
**page 9**

### RESCUE ME

With new malware becoming increasingly complex and a developing trend towards malware that prevents AV software from functioning, good rescue solutions have become vital. Andreas Marx looks at a range of end-user products.
**page 14**

### vbSpam supplement

This month: John Graham-Cumming reports on different ways to say 'Viagra' and Pete Sergeant presents his monthly summary of postings to the ASRG mailing list.

ISSN 0956-9979

*'The future of corporate malware support may very well lie in the outsourced engineer.'*

**Kenneth Bechtel**
Team Anti-Virus, USA

## OUTSOURCING: THE FUTURE OF ANTI-MALWARE SUPPORT?

Recently there has been a lot of discussion in trade magazines about businesses outsourcing their computer security. Many see it as inevitable that corporate computer security will be handled this way in the future: the business does not have the cost of maintaining a staff of high-salaried specialists, but enjoys the benefit of having the relevant expertise available as and when required.

For the firms providing the outsourcing service, one employee will be able to support 10 to 15 clients (in some cases more). The smarter of these firms will take on a small cadre of experts and build a team of less expensive 'technicians', who can support the client around the experts.

What does this have to do with the anti-virus world? Although I hate to say this, anti-malware management is one of the easiest components for a corporation to outsource.

While an anti-malware consultant needs to have the same level of access to company-sensitive data that a full-time employee would have, they do not need access to 'the keys to the kingdom' if sample handling is configured correctly. In the rare case that the consultant needs to visit a machine, non-disclosure agreements, and supervision by a member of staff will meet the trust requirements of the client.

While the prospect of outsourcing anti-malware support may seem to pose a danger to the job security of those in the line of corporate support, I believe it will be of benefit to us all.

Large corporations that can afford anti-malware staff will not be willing to let go of them (and, more importantly, the control they have over those staff). However, small- to medium-sized companies who do not have the budget to support a full-time team of anti-malware staff can leverage the expertise an outsourced group of specialists would provide.

How many times have we heard that it's the small and medium-sized businesses that are most affected by the current malware threat? It's a continuing cycle; companies pay a local consultant, who installs his favourite anti-virus software and sets it to auto update, but fails to manage the software.

Several small companies may like the idea of having someone manage their security for them, but do not like the fact that most of the anti-malware services available only check email, or support only a single vendor.

Outsourcing is also an attractive proposition for those larger corporations in which cost cutting is the rule – for the same reasons as it is for the smaller companies. For day-to-day maintenance and administration, a low-cost, entry-level employee can be hired, while the input and knowledge of an expert can be retained for less than it costs to maintain such an expert on site.

The outsourcing of computer security may be seen as both good and bad for the anti-malware industry as a whole. On the positive side, there will be more uniform anti-malware protection across all business levels, and quality research consultants will be coveted.

On the negative side, there is likely to be some consolidation, with a handful of individuals providing advice to a majority of the companies, potentially leading to a decrease in innovation and sharing of knowledge.

Overall, though, I feel that the trend towards outsourcing of anti-malware services is a positive one and the future of corporate malware support may very well lie in the outsourced engineer. Watch for a lot more consulting services offering anti-malware management over the course of the next year.

# NEWS

## PLANS, ACQUISITIONS AND ROYALTY

*Network Associates Inc.* (*NAI*) has unveiled plans to provide its customers with information and updates on software vulnerabilities. Initially the company will provide public statements on the severity of vulnerabilities, but it plans to expand the program into a comprehensive information service which will include real-time email alerts, daily summaries and web-based tools. Each vulnerability will be assigned one of five risk ratings ranging from 'low' to 'hyper-critical'. The level will be determined according to an estimate of the number of vulnerable machines, the likelihood that malware will be written to exploit the vulnerability and the potential for that exploit to travel widely via a worm. The initial phase of the program is scheduled to start in March/April 2004, with the more extensive service planned for later in the second quarter of this year. The company has not revealed whether the service will carry an additional charge for customers.

Last month *Symantec* completed the acquisition of management software manufacturer *ON Technology*. *Symantec* will incorporate *ON Technology*'s software distribution and configuration management capabilities into an end-to-end system designed to help customers build, manage, and protect their IT infrastructures.

February was also a busy month for *Sophos*: as well as opening its North American virus lab in Massachusetts, the company's UK-based global headquarters received a visit from Her Majesty the Queen and HRH Prince Phillip.

## GIGABYTE ARRESTED

Last month the Belgian Federal Crime Unit reported that they had arrested and questioned the virus writer known as 'Gigabyte'. Never one to shy away from the media spotlight (in fact, quite the opposite), Gigabyte's notoriety centres on the fact she is female – defying the ever-popular perception that virus writers are single males in their late teens to early twenties – and on her very public spats with *Sophos*'s spokesman Graham Cluley. She even went as far as to write two viruses (W32/Parrot and W32/Coconut) dedicated to him. The 19-year-old, who was held in custody overnight, was charged with 'computer data sabotage' and her five computers were confiscated. The website upon which she posted her viruses was also shut down. After several years of maintaining a very public profile and having written seven viruses – including W32/Sharpei, the first virus containing functional C# code (see *VB*, April 2002, p.4) – it is perhaps surprising that Gigabyte was not apprehended some time ago. If convicted the virus writer will face a prison sentence of up to three years as well as fines totalling up to 100,000 Euros.

### Prevalence Table – January 2004

| Virus | Type | Incidents | Reports |
|---|---|---|---|
| Win32/Mydoom | File | 72,431 | 71.31% |
| Win32/Bagle | File | 6739 | 6.63% |
| Win32/Opaserv | File | 6078 | 5.98% |
| Win32/Mimail | File | 5320 | 5.24% |
| Win32/Dumaru | File | 4251 | 4.19% |
| Win32/Swen | File | 1030 | 1.01% |
| Win32/Sobig | File | 998 | 0.98% |
| Win32/Dupator | File | 699 | 0.69% |
| Win32/Bugbear | File | 677 | 0.67% |
| Win32/Klez | File | 667 | 0.66% |
| Win32/Sober | File | 613 | 0.60% |
| Win32/Gibe | File | 363 | 0.36% |
| Win32/Yaha | File | 227 | 0.22% |
| Win32/Funlove | File | 212 | 0.21% |
| Win95/Spaces | File | 163 | 0.16% |
| Win32/SirCam | File | 155 | 0.15% |
| Redlof | Script | 73 | 0.07% |
| Win32/Fizzer | File | 73 | 0.07% |
| Win32/Lovsan | File | 73 | 0.07% |
| Win32/Lovelorn | File | 63 | 0.06% |
| Win32/Magistr | File | 58 | 0.06% |
| Win32/Nachi | File | 57 | 0.06% |
| Win32/Torvil | File | 47 | 0.05% |
| Inor | Script | 38 | 0.04% |
| Win32/Sdbot | File | 31 | 0.03% |
| Win32/Deborm | File | 26 | 0.03% |
| Win32/Ganda | File | 26 | 0.03% |
| Win32/Hybris | File | 24 | 0.02% |
| Fortnight | Script | 22 | 0.02% |
| Win32/Gaobot | File | 22 | 0.02% |
| Win32/Parite | File | 20 | 0.02% |
| Win95/Lorez | File | 18 | 0.02% |
| Others | | 281 | 0.28% |
| Total | | 101,575 | 100% |

[1]The Prevalence Table includes a total of 281 reports across 83 further viruses. Readers are reminded that a complete listing is posted at http://www.virusbtn.com/Prevalence/.

# VIRUS ANALYSIS 1

## HOW DUMARU?

*Peter Ferrie*
Symantec Security Response, USA

Take the SMTP client engine from W32/Mimail (see *VB*, September 2003, p.4), add some primitive social engineering in the email and some alternative-stream support from W2K/Stream (see *VB*, October 2000, p.6). Share the code freely so that others can add some backdoor capabilities and disable and/or remove other features. The resulting mess could be the W32/Dumaru family.

While Dumaru is classified as a virus family, the only variants that infect files are .A, .B, .D, .J, .Q and .T. Variants .F, .O, .S, .U and .AA do not even replicate, since their email replication code is disabled; these are simply backdoor programs.

### AND I RAN ...

Dumaru variants .A, .D, .J and .T begin by attempting to run the host code stored in an alternative stream called 'STR'. The alternative stream exists only on the Windows NT File System (NTFS). Interestingly, Dumaru.B and .Q also infect files, yet neither runs the host. Perhaps the author(s) of those variants considered the action to be unnecessary. This causes little trouble, though, owing to a bug in the infection code (described below).

After running the host, if applicable, all known Dumaru variants check for the existence of an atom, in order to prevent multiple copies of the virus running at the same time. The name of the atom is 'Program12345' in Dumaru.A, .D, .J and .T. The name changed to 'Program12345678' in variants .B–.V (excluding .D, .J and .T), to 'Program123' in Dumaru.W, 'Stamm-4' in variants .Y and .AB, and 'Stamm-2' in the .Z variant. The virus exits if the atom exists already, otherwise the virus creates it.

All known variants of Dumaru copy themselves to a number of locations, using several filenames, and alter the system in several ways in order to ensure that at least one copy is executed whenever *Windows* is restarted. All known variants copy themselves to the '%system%' directory and create a value named 'load32' under the 'HKLM\Software\Microsoft\Windows\CurrentVersion\Run' key in the registry, to point to the copied file.

Dumaru variants .A–.X copy themselves as 'load32.exe'; variants .Y, .Z and .AB copy themselves as 'l32x.exe'. Variants .A–.V copy themselves to the '%windir%' directory as 'dllreg.exe', then create a value named 'run=', in the 'Windows' section of the '%windir%\win.ini' file, to point to the copied file. Under W*indows NT/2000/XP/2003*, this action is usually redirected to the 'Run' value under the 'HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon' in the registry, however this behaviour is controlled by the values in the 'HKLM\Software\Microsoft\Windows NT\CurrentVersion\IniFileMapping' registry key.

All known variants of Dumaru copy themselves to the '%system%' directory, and create a value named 'shell=', in the 'Boot' section of the '%windir%\system.ini' file, to point to the copied file. Under W*indows NT/2000/XP/2003*, this action is usually redirected to the 'Shell' value under the 'HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon' key in the registry. Variants .A–.X copy themselves as 'vxdmgr32.exe'; variants .Y, .Z and the .AB variant copy themselves as 'vxd32v.exe'.

All known variants of the virus except for .A, .D, .J and .T query the 'Startup' value under the 'HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders' key in the registry, and copy themselves to the directory listed there. All of those variants prior to Dumaru.Y copy themselves as 'rundllw.exe'; variants .Y, .Z and Dumaru.AB copy themselves as 'dllxw.exe'.

### DROP AND GIVE ME TEN

At this point, Dumaru.A, .D, .J and .T create a file called 'windrv.exe' (if it did not exist already) in the '%windir%' directory, then run the file. This file is an IRC Trojan of limited capabilities (and not of sufficient interest to be described in detail here). All other known variants of Dumaru, except .L, .V, .Y, .Z and .AB, also carry this Trojan, though these variants will place it in a file called 'windrive.exe', and drop it at a later stage in their execution.

After dropping the 'windrv.exe' file, Dumaru.A, .D, .J and .T enumerate all drives from C: to Z:, looking for drives that are not CD-ROMs. For each such drive that is found, the virus changes to the root directory of that drive, and searches recursively for files whose suffix is 'exe'.

While performing the search, the virus skips the first entry in every directory. Although this is usually the '.' directory, this is not always the case (never for the root directory itself, and depending on the sorting order that is in use for subdirectories). Another bug exists in this code – since the search code in the virus does not change the current directory, a full path is required to access the file. In fact, the virus constructs the full path as required, but then passes only the filename to the infection routine. The result is that only files in the root directory can be infected.

The infection marker used by the virus is the presence of the read-only attribute on the file, with no other attributes set. The virus does not infect files that have only this attribute set. However, this causes a number of problems for the

virus. The virus is interested only in *Windows* Portable Executable (PE) files, but compares only the first three bytes of the four bytes in the PE signature. While this is generally sufficient, it is not always so. If the file is of the PE format, the virus enables filesystem compression for that file, if it is supported, using the DeviceIoControl() API that has been part of NTFS since *Windows NT 3.51*. This is the infection marker for W2K/Stream.

The virus creates a temporary file in the current directory, whose name begins with 'str', copies the found file to this temporary file, and attempts to copy itself over the file it found. This action fails if the file was read-only with other attributes set.

In the event that the copy was successful, the virus creates a stream called 'STR' in the copied file, and writes the temporary file to there, then attempts to delete the temporary file. This action fails if the file was read-only with other attributes set. The entire infection code (apart from the infection marker) is based on code from the W2K/Stream virus.

## THE-MAIL

After infecting the files in the root directory, Dumaru.A, .D, .J, .T, .Y, .Z and .AB attempt to delete a file called 'winload.log' in the '%windir%' directory, then enumerate all drives from C: to Z: once again, looking for drives that are not CD-ROMs. For each such drive that is found, the virus searches recursively for files whose suffix is 'htm', 'wab', 'html', 'dbx', 'tbb' or 'abd'. The virus searches within these files for text that resembles email addresses. The code used to perform this search is identical to that used by the W32/Mimail family.

The virus stores each unique email address in the 'winload.log' file. Once the search has been completed, the virus waits for an active Internet connection. When one is found, the virus determines the email server name for each email address in the 'winload.log' file by performing a Mail eXchange (MX) lookup on the domain name, using the first DNS server known to the local machine, if available – otherwise the virus will use 199.166.6.2 (ns.execulink.com) for the DNS.

The code to perform this task is clearly written by someone else, in the style of the virus writer Zombie (see *VB*, March 2001, p.6). The code searches in memory for the address of certain APIs that are already freely available to the virus. There is additional code that is unused by all known variants of Dumaru, which would load ADVAPI32.DLL and NTDLL.DLL.

If the email server can be determined, the virus will send an email. For all known variants of Dumaru prior to .Y, the email appears to come from 'security@microsoft.com'; for Dumaru.Y, .Z and .AB, the mail appears to come from a *Hotmail* user.

The subject is usually 'Use this patch immediately !', except in variants .L, .O and .P, which have no subject, and Dumaru.Y, .Z and .AB, in which the subject is 'Important information for you. Read it immediately !'.

For all known variants of Dumaru, prior to .Y, the message body is:

```
Dear friend , use this Internet Explorer patch now!
There are dangerous virus in the Internet now!
More than 500.000 already infected!
```

For Dumaru.Y, .Z and .AB, the message body is:

```
Hi !
Here is my photo, that you asked for yesterday.
```

The boundary is always 'xxxx'. For all known variants of the virus prior to Dumaru.Y, the attachment name is 'patch.exe'; for Dumaru.Y, .Z and .AB, it is 'myphoto.zip', a Zip file that contains a stored copy of the virus, whose name is 'myphoto.jpg[57 spaces].exe'.

Variants .L, .O and .P also encode another copy of the exe file into a script that will execute using HTML format email. While sending mail, the virus writes mail server return codes to the console, however since the application uses the GUI subsystem, the texts are not displayed. Dumaru.A, .D, .J and .T exit after sending the emails.

## GOSSAMER THREADS

All other known variants of Dumaru are multi-threaded. Dumaru.B and .Q create seven threads (ftp, tcp, mail, infect, proxy, clip, kwm) at this time. Other known variants of the virus have the mail and/or the infect threads removed. Dumaru.P contains only the mail, clip and kwm threads; Dumaru.Z contains only the mail, clip and mouse threads (perhaps because it downloads a variant of W32/Spybot, which contains far more functionality).

The most likely reason for the removal of the infect thread from other variants of Dumaru is the fatal bug that exists, which causes the virus to terminate entirely.

If the virus has not crashed, and is not Dumaru.V, .X, .Y, .Z or .AB, it enumerates the running processes and terminates any process whose filename matches any in the list that the virus carries. The list is identical in all known variants of the virus that contain this code, with the exception of Dumaru.P, in which one name is not present on the list, and Dumaru.AA, in which several names are not present on the list.

After creating the threads, all known variants of the virus prior to .Y create a file called 'guid32.dll' in the

'%windir%' directory. This file is a key-logging DLL. In Dumaru.H, .L, .M, .N, .O and .P, the DLL has been 'processed' in a manner similar to one of the infection methods that is present in W95/ZMist (see *VB*, March 2001, p.6). In Dumaru.Y, .Z and .AB, the key-logging functionality remains inside the virus itself. It functions similarly to the mouse thread that exists in the .W variant.

If the virus dropped the key-logging DLL, then it attempts to change the log filename in the DLL from 'SilentLog.txt' to '%windir%\vxdload.log' – however, doing so results in the corruption of the filename, with the degree of corruption depending on the length of the *Windows* directory name. In any case, the virus loads this file and uses it to install a system-wide keyboard hook, allowing logging to continue to run even after the virus exits. It is at this point that the remaining variants of Dumaru wait for an active Internet connection, then drop and run the 'windrive.exe' file.

## HOW TYPE-ICAL

The virus enables keylogging now. The code contains placeholders for up to five words (11 in Dumaru.W, 18 in Dumaru.Y and .AB, and 8 in Dumaru.Z) for which to search in window titles. The presence of any of these words enables the key logging automatically. If no words are specified, then the virus logs keys for all windows.

Currently, only variants .H, .O, .P, .W, .Y, .Z and .AB check for specific words:

Dumaru.H checks for 'Bank', 'Banking', 'Logon', 'Westpac', 'gold'.

Dumaru.O checks for 'gold', 'bank', 'Logon', 'Bank', 'Money'.

Dumaru.P checks for 'e-gold', 'PayPal', 'eBay', 'Sign', 'Evocash'.

Dumaru.W checks for 'gold', 'WebMoney', 'WM Keeper', 'Fethard', 'fethard', 'bull', 'mull', 'PayPal', 'Bank', 'bank', 'cash'.

Dumaru.Y and .AB contain the same list as Dumaru.W, with the addition of 'Storm', 'e-metal', 'Keeper', 'Bull', 'ebay', 'localhost', 'Winamp'.

Dumaru.Z checks for 'e-gold Account Access', 'e-metal', 'bull', 'Bull', 'mull', 'PayPal', 'Bank', 'bank'.

For all known variants of Dumaru except .W, .Y and .Z, if the title of a window is the Russian equivalent of 'The entrance to WM Keeper', then the virus searches recursively on the A: drive for '.kwm' files, and writes the contents of each found file to a file called 'rundlln.sys' in the '%windir%' directory. Dumaru.W appears to be of German origin, so perhaps something specific to Russia is of no interest to the author of that variant. The .Y, .Z and .AB variants are all based on Dumaru.W, so the code is probably missing for the same reason.

Periodically, the virus constructs an email to send to certain email addresses. The content of the email varies between different variants of Dumaru, but always contains sensitive information, such as: the local machine's IP address; a list of passwords for the 'Far Manager' software retrieved from the 'HKCU\Software\Far\Plugins\FTP\Hosts' registry key; a WebMoney ID list retrieved from the 'HKCU\Software\WebMoney\Options' registry key; the 'vxdload.log' keylogger data file (although this will be empty because of the filename bug described above); the clipboard log file (see below), and the kwm log file (see below).

Dumaru.F, .S, .U and .AA send a list of ICQ numbers retrieved from the 'HKCU\Mirabilis\ICQ\Owners' registry key, and all files whose suffix is 'pwl' that were found by searching recursively in the '%windir%' directory.

Additionally, variants prior to Dumaru.Y drop and run a file called 'winimg.exe' in the '%windir%' directory. This file is a protected-storage password viewer. The file is run with the '/stext %windir%\rundllz.sys' parameter to force saving of the information to '%windir%\rundllz.sys'. The resulting file is sent, too. In Dumaru.Y, .Z and .AB, the protected-storage password viewing code exists in the virus itself, and the results are written directly into the email to send.

The delay before the virus sends the sensitive mail is variant-specific. The list follows:

| | |
|---|---|
| Dumaru.B, .F, .H, .M–.O, .S: | every 30 minutes |
| Dumaru.C, .G, .K, .L: | every 5 minutes |
| Dumaru.E, .U: | every 2.5 minutes |
| Dumaru.I: | every 3.3 minutes |
| Dumaru.P: | every 23.3 minutes |
| Dumaru.Q: | every 50 seconds |
| Dumaru.R: | every 30 seconds |
| Dumaru.V: | every 15 minutes |
| Dumaru.W: | every ~21 minutes (*[1]) |
| Dumaru.X–.Z, .AB: | every 20 minutes (*[2]) |
| Dumaru.AA: | every 3 minutes |

*(*[1]) Dumaru.W also sends the keylog file whenever the file size exceeds 300 bytes.*
*(*[2])Dumaru.Z also sends the keylog file whenever the file size exceeds 100 bytes.*

Dumaru.Z also checks for the existence of a value called 'mailsended' [sic] in the 'HKLM\Software\SARS' registry key, and sends the mail immediately if it is not present. After sending the mail, Dumaru.Z creates that registry value.

The recipients of the email are variant-specific. Additionally, most variants support the use of a file called

'email.dat' which contains a user-defined email address. In the absence of this file, the default address is used. The list of default addresses follows:

| | |
|---|---|
| Dumaru.B: | x1234512345@centrum.cz |
| Dumaru.C, .G, .I, .L: | shogunn@world-banking.org |
| Dumaru.E, .Q, .R: | spbstels@rol.ru |
| Dumaru.F: | kollektinfo@mail.ru |
| Dumaru.H: | davailave@yandex.ru |
| Dumaru.K: | test799@altern.org |
| Dumaru.M, .O: | bank_acc@oligarh.ru |
| Dumaru.N: | bank-acc@yandex.ru |
| Dumaru.P: | trojan@e-e-mail.com |
| Dumaru.S: | kollekt-info@mail.ru |
| Dumaru.U: | info@domenov.net |
| Dumaru.V: | collector100@mail.ru |
| Dumaru.W: | geomir@centrum.cz |
| Dumaru.X: | pizdatiy_email1@list.ru |
| Dumaru.Y, .Z, .AB: | anyname@btw.egold-hosting.com |
| Dumaru.AA: | 7653345@list.ru |

Most variants of Dumaru will perform the MX lookup on the recipient's email address for the sensitive mail, too. However, variants .F, .U and .AA carry a list of servers (mxs.mail.ru, mx1.yandex.ru, mxd.rambler.ru, relay.hotbox.ru, mail.xaker.ru and mail.xakep.ru) and Dumaru.Y and .Z carry a single server (pop.btw.egold-hosting.com) to contact.

Additionally, variants .F, .U and .AA log in to POP3 servers before contacting another server. Those variants connect to 'pop3.rambler.ru' as user 'x1234512345' before sending through that server. Dumaru.F logs in to 'pop.mail.ru' as user 'pere-ssilka' before sending through 'smtp.mail.ru'; Dumaru.U logs in to 'pop.domenov.net' as user 'support@domenov.net' before sending through 'smtp.domenov.net'; Dumaru.AA logs in to 'pop.mail.ru' as user '5567' before sending through 'smtp.mail.ru'. [*The passwords used to access the sites are not given here, since some of the sites are still running - Ed*]. Those variants also retrieve the SMTP Server name from the 'Internet Account Manager' hive in the registry, and attempt to send the mail using that server.

In case the email sending is unsuccessful, there exists the option to send the data via FTP. Only a few of the variants support this option, and the FTP site, username, and password, are variant-specific. The list follows [*again, passwords removed to protect the innocent - Ed*]:

| Variant | FTP site | Username |
|---|---|---|
| Dumaru.C: | ftp.calkopt.narod.ru | calkopt |
| Dumaru.G: | ftp.world-banking.org | cybercrime |
| Dumaru.M: | ftp.pcihotup.com | pcihotup |
| Dumaru.N: | fixletterop.com | fixlette |
| Dumaru.P: | mail-technic.com | ftp1475 |
| Dumaru.U: | 207.150.192.12 | domenov0 |

## FTP THREAD

The FTP thread listens on port 10000 for incoming connections and accepts commands from a remote machine. It behaves like an FTP server, sending appropriate messages, such as '220' (Service ready for new user) on connection. It accepts the following commands:

| | | | |
|---|---|---|---|
| user | list | rmd | quit |
| pass | cwd | rnfr | type |
| stor | retr | rnto | rest |
| port | stor [again] | dele | cdup |
| pwd | mkd | syst | |

The 'user' command simply returns '331' (User name okay, need password). The 'pass' command simply returns '230' (User logged in, proceed). The 'stor' command creates the specified file on the local machine, sends '150' (File status okay, about to open data connection), accepts files up to 1,000,000 bytes long, then sends '226' (Closing data connection. Requested file action successful).

The 'port' command accepts a port number (used by the 'list' and 'retr' commands below), then sends '200' (Command okay). The 'pwd' command sends the name of the current directory on the local machine.

The 'list' command connects to the remote machine on the port specified by the 'port' command, sends '150' (File status okay, about to open data connection), sends tree under current directory on the local machine, then sends '226' (Closing data connection. Requested file action successful).

The 'cwd' command sets the current directory on the local machine, then sends '250' (Requested file action okay, completed). The 'retr' command connects to the remote machine on the port specified by the 'port' command, sends '150' (File status okay, about to open data connection), sends specified file from the local machine, then sends '226' (Closing data connection. Requested file action successful).

The 'stor' command would behave as the first 'stor' command does, but with a file size limit of 512 bytes. However, the command is not accessible because of the duplicated name.

The 'mkd' command creates the specified directory on the local machine, then sends '257' (<PATHNAME> created). The 'rmd' command removes the specified directory from the local machine, then sends '250' (Requested file action okay, completed).

The 'rnfr' command assigns the destination filename for the file copy that is performed by the 'rnto' command below, then sends '350' (Requested file action pending further information).

The 'rnto' command renames the specified file on the local machine to the name specified by the 'rnfr' command above, then sends '250' (Requested file action okay, completed).

The 'dele' command deletes the specified file from the local machine, then sends '250' (Requested file action okay, completed). The 'syst' command sends 'system' information (always '220 111 Windows').

The 'quit' command sends '221' (Service closing control connection. Logged out if appropriate), and disconnects from the network, but the virus continues to run.

The 'type' command simply sends '200' (Command okay). The 'rest' command simply sends '350' (Requested file action pending further information).

The 'cdup' command changes to the parent directory on the local machine, then sends '200' (Command okay).

## TCP THREAD

The TCP thread listens on port 1001 for incoming connections and accepts the following commands from a remote machine:

| | | | |
|---|---|---|---|
| !exec | !cdopen | !sndplay | !screen |
| !quit | !cdclose | !msgbox | |

The '!exec' command runs the specified file on the local machine. The '!quit' command disconnects from the network, but the virus continues to run.

The '!cdopen' command opens the CD-ROM drive door on the local machine. The '!cdclose' command closes the CD-ROM drive door on the local machine.

The '!sndplay' command plays the specified sound on the local machine. The '!msgbox' command displays a messagebox with the title 'THIS MACHINE IS CRACKED' and the specified message body. The '!screen' command saves the screen display to the specified file on the local machine.

Most variants of Dumaru support an additional command called '!email'. The '!email' command writes the specified address to 'email.dat' file in the '%windir%' directory.

## PROXY THREAD

The proxy thread listens on port 2283 for incoming connections. If a received packet begins with the number '4' then the number '1', the virus connects to the specified IP address on the specified port and acts as a proxy for the remote machine.

## CLIP THREAD

The clip thread copies small clipboard data (anything that is smaller than 32 bytes in length) to a file called 'rundllx.sys' in the '%windir%' directory.

## KWM THREAD

The kwm thread begins by checking for the existence of a file called 'rundlln.sys' in the '%windir%' directory. If the file does not exist, the virus enumerates all drives from C: to Z:, looking for drives that are not CD-ROMs. For each such drive that is found, the virus searches recursively for files whose suffix is 'kwm'. Dumaru.W also searches for files whose name is 'fethard_keyfile' or 'account.cfg'. The virus writes the contents of each found file to the 'rundlln.sys' file.

On completion of the search, the virus creates a key under the 'HKLM\Software' registry key, then writes a value called 'kwmfound', containing '0' if no files were found, otherwise it writes '1'. For most known variants of Dumaru, this key is called 'SARS', however it is called 'AAAA' in Dumaru.O, and 'MSDRV' in Dumaru.P.

## IRC THREAD

Dumaru.O and Dumaru.X contain an additional thread that connects on port 6667 (the default for IRC) to a certain channel on an IRC server. For Dumaru.O, the server is 64.191.107.10 (secure.timebase.us) and the channel is 'sars'; for Dumaru.X, the server is 'irc.wonka.net' and the channel is 'cooldman'. In either case, the virus joins the channel using a random nickname. The virus accepts the following commands via 'PRIVMSG':

| | | |
|---|---|---|
| download | email | stopdos |
| whois | dos | sendlogs |

The 'download' command downloads and runs a file from the specified URL. The 'whois' command sends the local machine's IP address to the channel.

The 'email' command writes the specified address to 'email.dat' file. The 'dos' command connects to the specified site, then sends empty 4kb packets as quickly as possible, until told to stop by using the 'stopdos' command. The 'stopdos' command stops the denial-of-service (DoS) attack started by the 'dos' command above. The 'sendlogs' command sends the sensitive mail as a file to the specified FTP site.

## MOUSE THREAD

Dumaru variants .W, .Y and .AB contain an additional thread that watches mouse events. When the left mouse button is pressed, the virus checks the window title of the current window. If the title matches 'C:\DATA\SRK.HTA' for Dumaru.W, or 'https://www.e-gold.com/srk.asp - Microsoft Internet Explorer' for Dumaru.Y and .AB, then the virus will capture the screen to a file whose name is a sequential number that begins at zero.

## CONCLUSION

It was interesting to see the variants of Dumaru evolve over time, from a mass-mailing virus to 'simply' a backdoor program (albeit quite a complex one).

Despite the apparent number of different authors among the variants, the basic functionality of the virus did not change significantly. Apparently, not one of them seems to know about the existence of the strcat() function to concatenate strings. Just how dumarthey?

### W32/Dumaru

| | | |
|---|---|---|
| Type: | Win32 SMTP mass-mailer worm. | |
| Size: | 9,216 bytes (A) | 34,818 bytes (O) |
| | 34,304 bytes (B) | 32,283 bytes (P) |
| | 36,354 bytes (C) | 34,308 bytes (Q) |
| | 9,220 bytes (D) | 36,352 bytes (R) |
| | 36,352 bytes (E) | 31,744 bytes (S) |
| | 31,744 bytes (F) | 9,240 bytes (T) |
| | 36,352 bytes (G) | 31,800 bytes (U) |
| | 34,304 bytes (H) | 31,232 bytes (V) |
| | 36,354 bytes (I) | 53,248 bytes (W) |
| | 9,220 bytes (J) | 34,304 bytes (X) |
| | 36,354 bytes (K) | 17,370 bytes (Y) |
| | 32,768 bytes (L) | 14,450 bytes (Z) |
| | 34,305 bytes (M) | 31,744 bytes (AA) |
| | 34,305 bytes (N) | 47,616 bytes (AB) |
| Payload: | Steals information, denial of service. | |
| Removal: | Fix registry, delete worm copies and its data files. | |

# VIRUS ANALYSIS 2

## WE'RE ALL DOOMED

*Gabor Szappanos*
VirusBuster, Hungary

'The crisis in Hungarian soccer deepens at almost the same rate as the Mydoom worm destroys computer systems.' This quote is from a Hungarian daily sports newspaper. Nothing I have come across illustrates the impact of this virus better – and the extent to which it has infiltrated everyday life.

The first identified sample of Mydoom came from Russia, which is the suspected origin of this virus. According to *MessageLabs*, about 1.2 million samples were detected during the first 24 hours of the virus spread – which overtook the previous record holder, Sobig.F, by a narrow margin. During the peak, 1 in 12 emails were infected with Mydoom.A – also a new record.

The first alerts on Mydoom arrived on Monday 26 January 2004, at around 10pm local time. Having spent a busy weekend fighting the Dumaru.Y outbreak (see p.4), I felt the name of this virus was completely justified.

## OVERVIEW

The virus usually spreads via email, but it can also spread using the *Kazaa* file exchange network. Mydoom.A is a 22,528-byte UPX compressed program. It uses a simple ROT13 algorithm to encode the most sensitive string variables in the virus code. The username and server name pool is not encrypted, but the registry locations, SMTP command and the message bodies are.

Upon execution the virus checks for the existence of the 'SwebSipcSmtxS0' mutex to ensure that only one instance of the virus runs at any one time. To indicate that a system is already infected, the virus creates the registry entry:

HKLM\Software\Microsoft\Windows\CurrentVersion\0Explorer\ComDlg32\Version

If this key is not present the virus launches a separate thread that creates a file with the name 'Message' in the %Temp% directory. The file contains nonsensical text (using characters between 16 and 255 ASCII code) and displays in the *Notepad* text editor. The virus generates 4096 characters for the file, but the actual size of the file is larger and varies, because line breaks are inserted (CRLF) randomly within the text.

After the editor window has been closed, the virus deletes this file.

The virus drops its backdoor component SHIMGAPI.DLL into the *Windows* system folder, and loads this library immediately.

At this point the worm checks the system date. If it is later than 12 February 2004, 02 hours 28 minutes 57 seconds UTC, no more of the virus's actions will be executed: it will not spread or run the DoS attack. However, it is only at this point that the date is checked, so if the worm instance was started before the drop-dead date, it will not stop working when the time passes this limit – the change will take effect only on the next startup.

Next the virus copies itself into the *Windows* system folder as TASKMON.EXE. The worm creates the key 'TaskMon=%System%\taskmon.exe' under the registry location:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

to ensure that it will execute automatically on *Windows* startup.

If the virus cannot create the key here (because of a lack of user privileges), it creates the key under the location

HKEY_CURRENT_USER\Software\Microsft\Windows\CurrentVersion\Run

## MAILING

In order to spread via email the virus gathers addresses from the *Windows* Address Book and from files with the extensions .htm, .sht, .php, .asp, .dbx, .tbb, .adb, .pl, .wab and .txt. The files are searched in the web browser cache and on all local hard drives. The addresses are stored in memory, rather than being saved to a local file.

The address gathering and the mail sender routines run in separate threads, with several memory variables synchronizing between them.

The subject line of the outgoing messages may be one of the following:

| | |
|---|---|
| test | Mail Transaction Failed |
| hi | Server Report |
| hello | Status |
| Mail Delivery System | Error |

The message body is one of the following (or, depending on the value of a random variable, random characters):

- Mail transaction failed. Partial message is available.
- The message contains Unicode characters and has been sent as a binary attachment.
- The message cannot be represented in 7-bit ASCII encoding and has been sent as a binary attachment.

This is a clever twist of social engineering: the virus doesn't even attempt to make itself look interesting. Instead, it camouflages itself as an error message, with the main content of the message attached. As the virus executable has the same icon as *Notepad* text documents, the unsuspecting recipient may think it is safe to open the attachment. In fact, the attachment is the virus with extension .bat, .exe, .pif, .cmd or .scr.

Occasionally it can create a ZIP package containing the virus (stored without compression) and send it as an attachment. In this case, the ZIP header contains the name of the executable in the archive, therefore the length of the header – and consequently the length of the archive – varies, despite the fact that the executable inside the archive is the same in all cases.

The filename of the attachment may be one of the following:

| | | |
|---|---|---|
| document | text | test |
| readme | file | message |
| doc | data | body |

The worm avoids sending itself to email addresses that contain the following strings (these domains are annotated in the virus source as being friendly domains):

| | | |
|---|---|---|
| "berkeley" | "kernel" | "ripe." |
| "unix" | "linux" | "isi.e" |
| "math" | "fido" | "isc.o" |
| "bsd" | "usenet" | "secur" |
| "mit.e" | "iana" | "acketst" |
| "gnu" | "ietf" | "pgp" |
| "fsf." | "rfc-ed" | "tanford.e" |
| "ibm.com" | "sendmail" | "utgers.ed" |
| "google | "arin." | "mozilla" |

Another set of domains is also avoided, but these are not likely to be considered friendly, these are more likely to be domains that are better avoided:

| | | |
|---|---|---|
| "avp" | "sopho" | "ruslis" |
| "syma" | "borlan" | ".gov" |
| "icrosof" | "inpris" | "gov." |
| "msn." | "example" | ".mil" |
| "hotmail" | "mydomai" | "foo." |
| "panda" | "nodomai" | |

The worm also avoids sending itself if the username contains the following strings (thus avoiding mailboxes with owners who may be more careful than the average):

| | | | |
|---|---|---|---|
| www | someone | service | ntivi |
| secur | your | help | unix |
| abuse | you | not | bsd |
| root | me | submit | linux |
| info | bugs | feste | listserv |

| | | | |
|---|---|---|---|
| samples | rating | ca | certific |
| postmaster | site | gold-certs | google |
| webmaster | contact | the.bat | accoun |
| noone | soft | page | |
| nobody | no | admin | |
| nothing | somebody | icrosoft | |

Despite these limitations, the virus obviously found enough targets to enable its global epidemic. This is probably because it relies on sending itself to general users who tend to click on attachments without consideration, while the addresses it avoids are likely to belong to sysadmins, who may be more careful.

Depending on the value of a random variable, the worm may not use the harvested email address. Instead it combines the domain part of the address with one of the usernames in the following list:

| | | | |
|---|---|---|---|
| sandra | adam | jane | jose |
| linda | ted | bob | andrew |
| julie | fred | robert | sam |
| jimmy | jack | peter | george |
| jerry | bill | tom | david |
| helen | stan | ray | kevin |
| debby | smith | mary | mike |
| claudia | steve | serg | james |
| brenda | matt | brian | michael |
| anna | dave | jim | john |
| alice | dan | maria | alex |
| brent | joe | leo | |

Finally, the virus sends itself via SMTP, constructing messages using its own SMTP engine. The worm attempts to guess the recipient email server. First it probes the domain part of the email address then, if it fails, it prepends the following strings and issues a DNS query of that server for each:

| | | | |
|---|---|---|---|
| mx. | smtp. | mxs. | relay. |
| mail. | mx1. | mail1. | ns. |

If none of the queries is successful, or the virus fails to connect to the target SMTP server, it will use the locally defined SMTP server read from the registry.

The sender of the message is spoofed by the virus. One of the collected email addresses may be used for this purpose or, with a two per cent chance, the sender name will be a three- to five-character string with one of the following domain names:

| | | | |
|---|---|---|---|
| aol.com | msn.com | yahoo.com | hotmail.com |

This leads to all the usual problems caused by a virus outbreak. Not only did the virus generate an enormous number of infected messages, but even more were generated by misconfigured mail servers. First, many of the recipients were invalid addresses, either because they were generated randomly, or because the email address collecting routine of the worm is faulty (the routine only checks the '@' character – so, for example, the worm attempted to send itself to the address 'w32.zaushka@mm.zip' – without much success of course).

Some servers throw the message back to the spoofed sender, and another problem comes in the form of infection notification messages. Despite the fact that many of the most prolific mass mailers spoof the sender address, the majority of email gateways send infection notifications to the spoofed sender when an infected message is encountered.

Another advanced feature of email protection programs is to purge the messages that are known to be generated by mass mailers. Otherwise, if only the attachment is deleted, the message still comes through, increasing the number of useless messages; but without the attachment, it is not easy to filter them out.

## KAZAA SPREADING

The worm copies itself into the download directory of the *Kazaa* peer-to-peer file exchange program. The location is read from the value of the registry key 'HKCU\Software\Kazaa\Transfer\DlDir0'. It uses one of the following file names:

| | |
|---|---|
| winamp5 | strip-girl-2.0bdcom_patches |
| icq2004-final | office_crack |
| activation_crack | nuke2004 |
| rootkitXP | |

The extension is .PIF, .BAT, .SCR or .EXE.

## DENIAL OF SERVICE ATTACK

Between 1 February 2004 and 12 February 2004, Mydoom.A performs a denial-of-service (D0S) attack against the website www.sco.com.

Since the virus only checks the system date on startup, this action will not take place until the next startup of the infected computer within this time frame. Also, the attack will continue after the end date until the computer is rebooted (or the virus process is stopped, for that matter). The DoS attack takes place if the virus is started after 16:09:18 UTC.

The worm sends a GET request every millisecond to port 80 of the site being attacked. However, due to a bug in the virus code the attack will not begin on all infected computers after the start date. While checking the current date against the start date, the virus compares the two dwords separately, requiring each to be above the specified start date. Thus, even if the qword representing the current date is higher than the qword of the start date, the attack only starts if the low dword is higher as well. As the stored low dword of the attack is 0xbe9ecb00, the attack occurs on only about 25 per cent of the infected computers.

The same does not apply to the end-of-life date check, because if the high dword is later than the end date, the worm exits without checking the lower dword.

## THE BACKDOOR

The virus drops SHIMGAPI.DLL, which is a backdoor component listening on the first available TCP ports between 3127 and 3198.

The DLL itself is stored in encoded form within the virus body. It is used for two purposes:

1. To establish a path to download and execute file to the infected computer.
2. To establish a proxy.

The DLL registers itself via the registry key:

HKEY_CLASSES_ROOT\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InProcServer32 "(Default)" = %SysDir%\shimgapi.dll

The default value of this key is 'Webcheck.dll', which is a COM interface for web monitoring. With this modification the worm makes sure that the shimgapi.dll file is loaded into the address space of explorer.exe upon the next startup. On the first execution on an infected computer, the virus itself loads this library.

While searching for a free port, the backdoor starts from port 3127. If the port is not free, it waits for 400 ms and skips to the next port. If none of the ports up to 3198 are free, it waits another 800 ms and goes back to port 3127 to start the process all over again.

When an available port is found, the backdoor creates three threads that listen on that port. A counter increments on incoming connections. If only one free listener thread is available, the backdoor will open two more listener threads.

On incoming data the first byte serves as an ID. Only two values of this ID are supported in Mydoom.A. If anything else is sent, or an error occurs, an error status message is sent back.

If the ID is 85h, then four bytes are skipped, the next four bytes must match the magic dword 133C9EA2h. If this condition is true, the rest of the stream is saved into a temporary file and executed. An attempt was made to use this feature in Mydoom.B to update the systems infected with the original version of the worm.

If the ID is 4h, the rest of the stream is read, then the target IP address is extracted from the stream. If the backdoor can connect to the IP address, it acts as a proxy.

The first function enables an attacker to install a program of his will to the infected computer. All that needs to be done is to scan for these open ports, and then the computer is wide open for the attacker. Only a couple of days after the appearance of the virus there were already signs of port scans within this port region. Some of the scans were coming from sysadmins trying to find infected systems, but the volume of traffic seen was more than could be attributed to this source.

While the worm will not spread or perform the DoS attack if executed after the drop date, it will still create and execute the backdoor after its time has expired.

## TAKE TWO

A couple of days after the original, a modified variant of Mydoom appeared. Its functionality was similar to that of the .A variant, with slight modifications. Mydoom.B infests itself as EXPLORER.EXE.

The subject lines are:

```
Returned mail       Mail Transaction Failed
Delivery Error      Mail Delivery System
Status              hello
Server Report       hi
```

And the message bodies:

- `sendmail daemon reported:`
- `Error #804 occured during SMTP session. Partial message has been received.`
- `Mail transaction failed. Partial message is available.`
- `The message contains Unicode characters and has been sent as a binary attachment.`
- `The message contains MIME-encoded graphics and has been sent as a binary attachment.`
- `The message cannot be represented in 7-bit ASCII encoding and has been sent as a binary attachment.`

The filename of the attachment may be one of the following:

| | | |
|---|---|---|
| document | text | message |
| readme | data | body |
| doc | test | file |

The worm copies itself into the download directory of the *Kazaa* peer-to-peer file exchange program. It uses one of the following file names:

| | |
|---|---|
| icq2004-final | Winamp5 |
| Xsharez_scanner | AttackXP-1.26 |
| ZapSetup_40_148 | NessusScan_pro |
| MS04-01_hotfix | |
| BlackIce_Firewall_Enterpriseactivation_crack | |

Starting on 1 February 2004, Mydoom.B performs a denial of service attack against the website www.microsoft.com, and from 3 February 2004 against the website www.sco.com. The virus stops its activities upon the first system boot after 1 March 2004.

The virus modifies the hosts file to redirect the following websites to 0.0.0.0, thereby disabling access to them:

| | |
|---|---|
| ad.doubleclick.net | phx.corporate-ir.net |
| ad.fastclick.net | secure.nai.com |
| ads.fastclick.net | securityresponse.symantec.com |
| ar.atwola.com | service1.symantec.com |
| atdmt.com | sophos.com |
| avp.ch | spd.atdmt.com |
| avp.com | support.microsoft.com |
| avp.ru | symantec.com |
| awaps.net | update.symantec.com |
| banner.fastclick.net | updates.symantec.com |
| banners.fastclick.net | us.mcafee.com |
| ca.com | vil.nai.com |
| click.atdmt.com | viruslist.ru |
| clicks.atdmt.com | windowsupdate.microsoft.com |
| dispatch.mcafee.com | www.avp.ch |
| download.mcafee.com | www.avp.com |
| download.microsoft.com | www.avp.ru |
| downloads.microsoft.com | www.awaps.net |
| engine.awaps.net | www.ca.com |
| fastclick.net | www.fastclick.net |
| f-secure.com | www.f-secure.com |
| ftp.f-secure.com | www.kaspersky.ru |
| ftp.sophos.com | www.mcafee.com |
| go.microsoft.com | www.microsoft.com |
| liveupdate.symantec.com | www.my-etrust.com |
| mast.mcafee.com | www.nai.com |
| mcafee.com | www.networkassociates.com |
| media.fastclick.net | www.sophos.com |
| msdn.microsoft.com | www.symantec.com |
| my-etrust.com | www.trendmicro.com |
| nai.com | www.viruslist.ru |
| networkassociates.com | www3.ca.com |
| office.microsoft.com | |

One particular feature of Mydoom.B is worth mentioning. Using the file upload and execute feature of the backdoor component, the virus attempted to upgrade existing Mydoom.A infections with the new version. After activation it generated random IP addresses and attempted to upload itself to port 3127 of those systems. Fortunately and surprisingly, the .B variant did not spread well. While *MessageLabs* stopped over one million samples of the first variant on the first day, only eight samples of the second variant were found – which were most likely seeding samples.

There was also a bug in the DoS routine of the second variant. Due to a programming error (the same comparing error, coupled with another check), the attack against www.microsoft.com never occurs.

## AFTERMATH

The sheer number of infected computers with the backdoor installed was too tempting an opportunity to let pass. Around 1 million computers were waiting for someone to send them just about any code to execute. The author of Mydoom.A couldn't resist this temptation, and wrote a new worm, Doomjuice.A. This had only one propagation method, the 'Mydoom backdoor' method. It attempted to connect to port 3127 of random IP addresses then sent itself for execution. On infected computers it dropped an archive containing the (almost) complete source code for Mydoom.A. This worm also had a fixed date check in the DoS procedure, for attacking www.microsoft.com.

## CONCLUSION

Once again, a simple email worm hit the world. Mydoom did not use clever tricks or new exploits (in fact, not even old exploits) to launch its attachment automatically. It relied on the old click-and-run routine. It has been possible to configure *Outlook* and *Outlook Express* to block access to files with executable extensions for years. However, the majority of users do not bother to install the latest patches for these email clients and the vast majority of users have not learned the lesson of not clicking on attachments. We are bound to be doomed again in the future.

*[In next month's VB Gabor Szappanos will look at the worms that use the backdoor component of Mydoom to spread in 'Life after Mydoom'.]*

FEATURE

# RESCUE ME 2: DISINFECTION WITH BOOTABLE RESCUE MEDIA

*Andreas Marx*
AV-Test.org, Germany

These days, it is not an uncommon occurrence for a PC to become infected by a virus or worm, or for a backdoor to be installed on one's PC – at the time of writing, for example, *Trend Micro*'s free online virus scanner has found more than 1.6 million PCs infected with W32/Mydoom.A.

There is, and there always will be a time delay between the initial detection of a worm and the release of anti-virus definition updates (see *VB*, February 2004, p.4). Heuristics and the generic proactive malware detection techniques used by anti-virus products do not always work – for example, no AV scanner was able to detect W32/Sober.C or W32/Mydoom.A without updated signatures.

There may be an even longer delay between an anti-virus signature update being made available and the end user applying the update to his software. This is compounded by the problem that a lot of retail AV products for home users, such as *Norton AntiVirus 2004* and *McAfee VirusScan*, cannot be updated with non-administrator rights on *Windows XP*-based systems.

Malware infections can be rather complex. These days, it is not simply a case of removing a 'worm.exe' file (along with a registry key in the 'Run' section or an entry in the win.ini file – things a lot of anti-virus programs still omit to do). A lot of current malware threats, for example W32/Sober (see *VB*, December 2003, p.7), try to hide themselves from other applications or have self-protection mechanisms that prevent removal tools from working properly.

A number of current threats (for example, W32/Oror.C) attempt to deactivate or even delete any anti-virus software that is running on the infected machine – this is very easy considering that few anti-virus programs have any form of self-protection.

Some worms, like W32/Mydoom.B, change the *Windows* 'hosts' file so that certain websites cannot be reached. To my knowledge, no anti-virus program is able to check for (or remove) suspicious entries in the 'hosts' file. This means that the anti-virus product cannot easily be updated, and therefore is less likely to be able to detect the threat that has infected the PC.

It is essential, therefore, to have a good rescue (and/or backup/restore) solution that does not rely on the infected *Windows* system. This article – which is an update to the 'Rescue me' article in the May 2002 issue of *VB* (see *VB*, May 2002, p.10) – focuses on end-user products.

Some recovery solutions can be started from the installation CD, while others need to be created manually. This may call for up to nine disks in the case of *Norton AntiVirus* or a single CD-R/RW in the case of *G Data AntiVirusKit (AVK)*. Here, the CD image with up-to-date signatures is created using Mkisofs and burned using Cdrecord, both of which are available as free software for *Windows* (see http://www.fokus.gmd.de/research/cc/glone/employees/joerg.schilling/private/cdrecord.html). Maybe we will see rescue USB sticks in the not too distant future.

Today's rescue solutions can be classified into three main categories: DOS, *Linux* and *Windows* (*PE*)-based. In most cases, NTFS is supported only in read-only mode.

## DOS-BASED SOLUTIONS

Most rescue media, like those from *Grisoft AVG*, *Command AntiVirus*, *Computer Associates eTrust*, *McAfee VirusScan* and *Norton AntiVirus*, are still based on DOS. This is useful if one wants to disinfect a boot virus, which is not possible when *Windows NT*-based systems are running because they deny access to this critical boot area. However, DOS incarnations support only FAT16 or FAT32 drives (e.g. FreeDOS, http://www.freedos.org/, or MS-DOS).

Some tools, such as *Norton AntiVirus*, claim that they have scanned all hard drives and found no infected files, despite the fact that the system only has NTFS drives which the product cannot scan at all.

Another problem is that most DOS-based rescue systems are extremely outdated. For example, the installation CD of *Norton AntiVirus 2004* from September 2003 is bootable, but contains signature files dating from mid-2001. The rescue disk that a user can create in *McAfee VirusScan* boots 'Dr Solomon's Magic Bullet' (the doctor has not left town, he is still alive!) with signatures from March 2000.

There are NTFS add-on drivers available, such as Winternals (NTFSDOS/NTFSDOS Professional, http://www.winternals.com/) or Active Data Recovery Software (NTFS Reader for DOS, http://www.ntfs.com/), but in the freeware editions they are only able to provide read-only support, and the products with both read and write support usually cost more per licence than the anti-virus product itself. In most cases, only file access is allowed, but the *Windows* registry cannot easily be modified.

Furthermore, memory limitations mean that it is almost impossible to get network drivers and a TCP/IP stack (for product updates) as well as the NTFS drivers, plus the AV program running at the same time. Therefore, DOS is no longer a good solution for scanning or cleaning if one is dealing with more than a boot sector or master boot record.

## LINUX-BASED SOLUTIONS

The number of *Linux*-based rescue solutions has increased considerably over the last couple of months. *Central Command Vexira Antivirus* (available free of charge as an ISO image at: ftp://ftp.centralcommand.com/antivirus/rescue_disk/), *G Data AVK*, *BitDefender*, *H+BEDV AntiVir Professional*, *Kaspersky Anti-Virus*, *Norman Virus Control* and *Panda AntiVirus* are all based on *Linux*.

The good news is that *Linux* has no problems with read and write access to FAT16 or FAT32 drives. Read-only access to NTFS drives works too, however there are a couple of problems with write access to NTFS drives.

*AVK* is still based on *Linux* kernel 2.2.14 and it uses a 1998 beta version of *Kaspersky*'s *AVP* for *Linux* to scan a system. Unfortunately this old kernel cannot handle *Windows 2000* and *XP* NTFS5 very well, and will crash on the first EFS-encrypted file. This old kernel also has problems with Serial ATA (SATA) drives: it simply will not see them.

*Kaspersky Anti-Virus* and *Panda AntiVirus* are based on 2.4.x kernels with a minimal *Linux* system that fits on one floppy disk. *AntiVir* and *Vexira* are only slightly different: these products use a CD-R instead of a floppy disk.

*BitDefender* and *Norman Virus Control* are based on *Knoppix-Linux* (http://www.knopper.net/), a *Linux* distribution that can be started completely from the bootable installation CD. *Knoppix* attempts to detect all attached devices automatically and load the correct drivers. It works with both the 'older' 2.4.x and the more up-to-date 2.6.x *Linux* kernels. While the original *Knoppix* distribution includes several additional applications such as *OpenOffice*, the *BitDefender* version includes only the graphical user interface KDE (Kommon Desktop Environment, http://www.kde.org/) and the scanner itself. *Norman* has reduced the *Knoppix* installation even further, with its system based on a text console only.

However, even if NTFS drives can be read and scanned for malware, there is still the problem that infections cannot be removed. The NTFS drivers in the latest *Linux* kernel 2.6.x (http://linux-ntfs.sourceforge.net/) are good enough to replace files with other files safely if both files have the same name and length. Therefore, it's possible to remove 'malware.exe' and replace it with a helper file that completely repairs the system when *Windows* starts. This way, registry keys can easily be repaired as well.

Most of today's malware files are big enough to accommodate being replaced with well-working cleaner utilities. In order to make sure the replacement file has the same size as the malware being replaced, the rescue AV tool can simply add a few 0x00 or random bytes at the end. Another option would be to replace the 'malware.exe' file with a special file that triggers the detection of the *Windows* part of the AV program and the files can be successfully cleaned as well.

An alternative method that would avoid all these problems would be the use of *Captive* (http://www.jankratochvil.net/project/captive/), a free, fully-read/write NTFS driver for *Linux*. It uses the *Linux* kernel NTFS drivers to read the ntfs.sys and a few other *Windows* system files and finally it loads the native *Microsoft* NTFS driver. A more detailed description of the process can be found at http://www.amunra.co.uk/archives/000028.php.

Use of the native *Microsoft* drivers is a good way to avoid all the compatibility problems with the undocumented features of NTFS, but one should keep in mind that it's not a trivial task to load *Windows* drivers on *Linux*. For example, the *BitDefender* rescue media uses *Captive* to gain read and write access to NTFS partitions, but the beta version we used for testing was not yet able to remove a malware file from NTFS drives – probably due to a bug in the 'disinfect' or 'delete' program options.

If one uses *Linux*, the rescue media can be updated very easily: with all of the built-in drivers, it is easy to get a network card running in order to download updates from http or ftp sites, from SMB shares of other computers or even to grab the definition files which are stored on the HDD already.

## WINDOWS (PE)-BASED SOLUTIONS

All of the aforementioned rescue tools share the problem that they are based mainly on reverse engineering of the file systems, regardless of whether they are FAT or NTFS, or that a lot of work-arounds and tricks need to be employed in order to get them working.

*Microsoft* has its own *Windows*-based solution, *Windows PE*, which can be started from a read-only medium, such as a CD-Rom. A lot of backup and rescue tools such as *Winternals Administrator's Pak* (http://www.winternals.com/products/repairandrecovery/) or *Symantec*'s *Powerquest V2i Protector* (http://www.powerquest.com/v2i/protector/sbe/) use *Windows PE* already.

*Alwil Software* has created the BART CD (Bootable Anti-Virus and Recovery Tools – see http://www.asw.cz/), which is also based on *Windows PE*. This not only includes a virus scanner which is able to read and write NTFS partitions without any problem, but it contains a disk checker, a registry editor, a file manager, plus a text editor.

All of these tools share one problem however: while they are easy to develop, because they are based on *Windows* and support most parts of the *Windows* API, they are also

expensive, because *Windows PE* licences are neither cheap nor easy to obtain.

It is possible that Bart Lagerweij thought of this when he developed *PE-Builder* (http://www.nu2.nu/pebuilder/), which is similar to *Windows PE*, but is free. Lagerweij used a number of components of the original *Windows PE* system in the first version of *PE-Builder* but, at *Microsoft*'s request, removed this version from his website. According to the author, today's versions are fully legal – as long as the user creates his own, personal CD from his own computer's *Windows XP* (SP1) or *Windows Server 2003* system. Lagerweij has developed his own additions and tools in cooperation with other developers worldwide and, in some areas, *PE-Builder* provides much more functionality than *Microsoft*'s own *Windows PE* (see http://www.www.nu2.nu/pebuilder/#plugins for details).

However, not all programs will run on *Windows PE* – in particular the more complex tools have problems. *SureBoot* (available for a 'rather small' licensing fee, see http://www.sureboot.com) could solve this problem. *SureBoot* can automatically create a backup copy of a user's specific *Windows 2000/XP* environment (including all drivers, specific user profiles, and AV/backup software), which boots and runs *Windows* from a hidden hard disk directory and can be burned onto a CD/DVD. Complex applications such as *Word*, *Excel*, *Outlook* and *IE* work as well.

After an infection, the virus definitions can be updated using standard *Windows* Internet connection services. The infected, non-running, but accessible *Windows* system can then be repaired directly from *SureBoot* with full NTFS and registry read and write capabilities, based on *Microsoft*'s own drivers. Most applications will run without problems and they won't see any differences, regardless of whether they are working on a real *Windows* system or a *SureBoot*-created rescue CD/DVD. Unfortunately, this solution is likely to be 'too big' for AV-only rescue media – but, combined with other rescue and administration tools, it could be very useful.

## CONCLUSION

Recently malware has increased in complexity. The cleaning of an infected PC is becoming a harder task, especially if the malware 'kills' the AV product or prevents it from updating itself. We need better rescue solutions urgently. Today's DOS-based disks won't work any more, due to the lack of NTFS support. There are still lots of *Windows 9x/Me* systems in use that can be disinfected successfully. However, the number of *Windows 2000* and *XP* installations is growing fast and with it, the use of NTFS as the standard file system. I hope that we will see more really innovative products like *Alwil*'s BART CD in the near future.

# CALL FOR PAPERS

## VB2004 CALL FOR PAPERS: DEADLINE 31 MARCH 2004

*Virus Bulletin* reminds those wishing to submit papers for a presentation slot at VB2004 that the deadline for abstract submissions is **31 March 2004**.

Submissions are invited on all subjects relevant to anti-virus and anti-spam.

The following is a list of suggested topics elicited from attendees at VB2003. This list is *not* exhaustive and papers on these and any other AV and spam-related subjects will be considered.

- Hardware AV solutions.
- Detailed discussion of the latest viruses.
- Control of web-based transmission of malware.
- P2P threats.
- Vulnerabilities and patch management.
- AV engine architecture.
- Hoaxes and spam from a legal point of view.
- Malware intelligence gathering and legal issues associated with catching virus writers.
- Forensics: tools, techniques, reading IP headers etc.
- Virus/worm traps on internal networks.
- Threats relating to the *.NET* framework, *IIS6.0,* XML.
- *Linux* security issues.
- Corporate case studies of single virus incidents.
- Corporate case studies of spam management.
- Implementing a successful corporate AV strategy.
- Integrating anti-virus, anti-spam, IDS and other security software.
- Prevention of fast-spreading, 'Slammer-like' malware.
- Use of VMware for malware testing.
- Security issues relating to PDAs and mobile phones.
- Central management of anti-virus (e.g. ePO).
- Codes of ethics for users.
- Corporate end-user/virus response team training.
- Spyware, RATS, adware, hacker tools, DoS tools.

Abstracts of approximately 200 words must be sent as RTF or plain text files to **editor@virusbtn.com** no later than Wednesday 31 March 2004.

VB2004 will take place 29 September to 1 October 2004 at the Fairmont Chicago, Illinois, USA. For full information and online registration see http://www.virusbtn.com/.

# PRODUCT REVIEW

## GRISOFT AVG 7.0

*Matt Ham*

*Grisoft*'s *AVG* has been a regular entrant in the *VB* comparative tests for many years, with two major version updates in my time as a reviewer. The more recent of these version changes was first examined by *VB* in the comparative review on *Windows NT 4* (see *VB*, February 2004 p.12). Regretfully the comments made in that review were based on a rather more hurried testing process than usual and, as a consequence, some statements need to be amended and the record set straight. In short, *AVG 7.0* does have the ability to create larger logs and to deal with multiple infections automatically.

However, instead of producing an erratum to rectify the situation it was decided that, in this case, a full-scale review of the product was in order.

*Grisoft* is based in the Czech Republic and specialises only in anti-virus software. No other products are advertised either on the company's website or in the product's documentation – something of a rarity these days when expanded product ranges are de rigeur amongst anti-virus companies.

### DOCUMENTATION AND WEB PRESENCE

Unusually, the product was supplied as a boxed version complete with manual. The box contained a jewel-cased CD, installation manual and a registration card. The box itself seemed rather more eye-catching in design than many of the other products on the market – which can be explained by the fact that *AVG* is designed for sale to home users as well as to corporate customers.

The CD contains a number of versions of *AVG 7.0*, older version 6.0 files, documentation, anti-virus utilities and some trial versions of other software. The versions of *AVG 7.0* available are *Professional*, *Network Edition*, *Email Server Edition*, *File Server Edition* and *Linux Edition*. The *Network Edition* offers remote administration and installation via the installation of the *AVGADMIN* utility. Email server software supported by the product includes: *Microsoft Exchange*, *Lotus Notes/Domino*, *Kerio Mail Server* and *602 Lan Suite*.

The manual provided is by no means a complete guide to the operation of the software, being focused instead on the installation and initial configuration of *AVG*. The sections on virus removal and general troubleshooting are well written and address several issues which tend to confuse less expert users (e.g. the reasons why some viruses cannot be disinfected). Given that there are many different versions available when different language and platform combinations are considered, this minimal hard copy documentation certainly cuts down on production and transport costs.

Documentation files on the CD are rather hidden away, scattered in the tree structure of the CD. This was surprising, as the product documentation is one feature which one would expect to be as easy to find as possible.

Happily, documentation is available and easy to access when installing the product – here it appears in PDF format, with *Acrobat Reader* available on the CD. Although *Linux* versions of the product are present on the CD, a *Linux* version of *Acrobat Reader* is not provided – a small, but potentially irritating oversight.

In the case of *AVG Professional* the content of the electronic documentation was identical with that of the hard copy manual, resulting in an absence of advanced documentation as far as this version of the boxed product is concerned. The documentation for other platforms was of a more advanced nature, which is something of a necessity when dealing with mail servers and distribution across a network.

*Grisoft*'s website is located at http://www.grisoft.com/. The site is less sprawling than many other anti-virus vendor sites and offers speedy access to all contents – these being the usual downloads, tech support, virus-related information and news sections. Within the documentation section of the website the files available are identical to those on the CD, with the exception of one: the executable file to install full online help within the program. The lack of any more advanced manuals is a little worrying, but since this version of the product is still very new, it is hoped that the manufacturer will remedy the situation in time.

This leaves the help that is accessible from within the *AVG* application itself. As installed without the additional executable file, this is very brief and mentions only basic functionality and concepts. Once the additional help data has been added the effects are not immediately obvious other than there being images in the help file. There are, however, additional details available in places, but the help file remains a little lacking on such information as relevant keyboard shortcuts.

### INSTALLATION AND UPDATE

Installation from the CD commences, as would be expected, with an autorun. This produces a choice of languages for the installation: Czech, Slovak, US English, UK English, German or French. UK English was chosen for all tests. Having carried out the last comparative review on a *Windows NT 4* installation, *Windows XP Professional* was selected this time. Installation of *AVG* is offered for the

versions mentioned previously; *AVG Professional* was selected for general testing purposes.

Having selected the application for installation the first option presented is whether a full or demo version will be installed. For other *AVG* versions the demo version is available only via the website. There was a slightly worrying delay in initialisation, followed by another list of installation languages from which to select. This list differs from the one offered via the initial autorun – if a user requires, for example, a Portuguese installation they will have to select a language other than Portuguese at the initial selection, before being able to select the desired language here. After accepting the terms of the licence agreement an initial check of the *AVG* files is followed by the input of registration codes before the main installation can proceed.

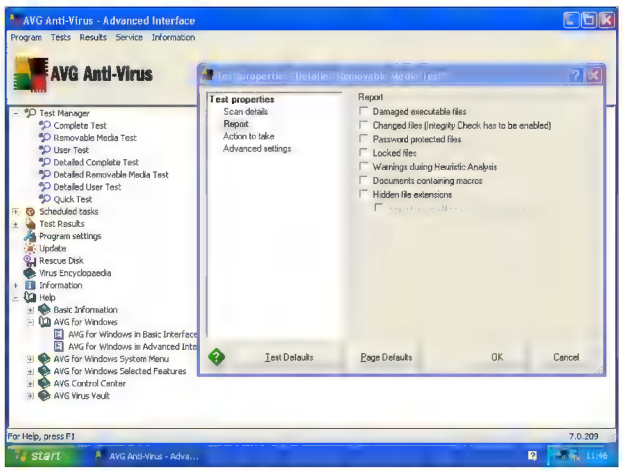
Component selection is rather novel in that it does not offer the usual default/advanced/custom trio – only a tree with check boxes for the components to be installed. By default, AVG Anti-Virus, Resident Shield, E-mail Scanner and Personal E-mail Scanner are activated. The only additional feature which may be enabled is the Remote Control Communication Library. It is possible to de-select any of these features, although some are dependent on others to operate. The Remote Control Communication Library, if installed, requires the parameters for *AVG*'s DataCenter, a function of the administrative utilities available. Other selections require no further details before installation can be completed.

After installation the *AVG* application is launched automatically. Initially this was accompanied by an alert from the task bar concerning the out-of-date nature of the virus definition files. Upon the automatic launch a selection of options are given, starting with updating. Updating may be performed manually, by placing the .BIN update files in the appropriate directory, or using the automatic update utility. Either method is quick and, in the case of those updates applied here, without snags.

Next comes the option to create a rescue disk and the option for a scan of the machine in question. At this point the installation is complete. Rescue disks may also be created at any later stage, which would be wise in the event that major system configuration changes are made.

## FEATURES

*AVG* is one of those anti-virus utilities which offers two separate interfaces, the Basic and Advanced versions. A more user-friendly front end is presented when the Basic interface is selected, while offering maximum flexibility. *Grisoft* offers a totally free version of *AVG* for non-networked, non-commercial home use, which is limited




*AVG Professional, Advanced interface.*

to this basic interface. The free version does not offer fully configurable scheduling or test creation and comes without technical support. The demo version, on the other hand, is full featured with access to technical support – but time-limited.

The full version with Advanced interface was selected for testing rather than these two more limited versions. This is in the almost standard tree structure rather than the button-oriented interface of the Basic interface. The Advanced interface offers a Test Manager, Scheduled Tasks, Test Results, Program Settings, Update, Rescue Disk, Virus Encyclopaedia, Information and Help areas.

The test manager comes with pre-configured scans for various purposes. Scans of all files, removable media or user-selected areas are offered in both a Standard and a Detailed form. The differences between the Standard and Detailed scans are that the former applies an integrity check, thus potentially saving time on subsequent scans, and scans by file type. Detailed scanning, on the other hand, scans all files without using integrity checking. Detailed scanning is thus expected to be considerably slower than the standard method. Both scan methods use heuristics and scan inside archives. In addition there is a pre-configured Quick Test which scans boot areas, registry and a small number of vital system files.

User-defined tests may also be specified, with numerous additional parameters. Reports are particularly configurable, with the ability to note seven statuses in addition to infected files, ranging from any documents which contain macros through to files which are locked and unable to be scanned. Action on detection can be set, although the choices here are limited to automatic disinfection or user selection from a dialog. Automatic disinfection does not occur at the point of detection, but after the scan has completed.

If user interaction is selected the options are Continue, Info, Heal, Delete File, Move to Vault and Stop. Unfortunately, however, there is no option to apply the same action to any subsequent files, only the option to scan remaining files without user interaction. In the case of multiple infections which are required to be treated in some way other than disinfection, therefore, the actions must be performed through the report interface.

The report interface gives a list of infected files, the result of scanning each of those files and the current status of those files. By right-clicking on multiple selections of files the option is given to disinfect, delete or quarantine the files to the Virus Vault. Oddly enough this selection of actions does not occur if single files are selected. All files may be selected for treatment here by use of the Ctrl-A hotkey, though there is no GUI method of performing this action and no mention of the hotkey in the help file. (It was this that resulted in the incorrect claims in the comparative review regarding multiple file deletions.)

The *Windows NT* comparative review stated that files cannot be exported. In fact this is possible through a drop down menu (which, unfortunately, is obscured by the Test Result window when viewed in maximised mode). When both of these mistakes were rectified the detection rate of *AVG* on demand returned to its usual excellent levels, with all files from the In the Wild test set being detected.

Construction of scheduled tasks is a simple affair, there being a varied selection of trigger situations. There is an option to trigger a scheduled job when an Internet connection is first established, which can be linked to an update task. Potentially this is most useful for a home user, though it will also be useful where users of laptops are concerned.

Various parameters may also be configured from the Program settings area. These include the interface itself as well as some short cut keys and numerous ways in which information is displayed. With such configurable interface options and test parameters it is perhaps not surprising that a basic interface was supplied, since many users would otherwise be confused by the depth of choice.

## CONCLUSION

On first use, *AVG 7.0* seemed to be a most frustrating beast. Having revisited the product a month later, however, the truth of the situation proved to be very different. The reasons behind the discrepancy are linked mainly with this reviewer having had a very lengthy acquaintance with *AVG 6.0*, and having gained habits which, when applied to the new version of the product, were not applicable and led to some false conclusions.

Despite there being a large degree of error between seat and keyboard, the changes to the program were not made as obvious as they could have been, and the documentation was not always helpful. However, documentation is significantly easier to update than an application and this version of the product is still relatively new, so it is not entirely surprising (although not entirely forgiveable) that the documentation is limited at this stage.

Matters of confusion aside, the product has been made more flexible in many ways and detection remains at its usual high levels. Only a few false positives, the source of which has been detected and dealt with, blotted the product's performance in the last comparative review once the tests had been re-run. *AVG* thus makes a welcome return to my list of 'easy-to-test' products, with the prospect of more VB 100% awards in the not too distant future.

**Technical details:**

**Product:** Grisoft AVG 7.0

**Test environment:** Identical 1.6 GHz Intel Pentium machines with 512 MB RAM, 20 GB dual hard disks, DVD/CD-Rom and 3.5-inch floppy drive running *Windows NT 4.0 SP6* and *Windows XP Professional*.

**Developer:** *Grisoft*, Lidicka 31, 602 00 Brno, Czech Republic; email sales@grisoft.com; website http://www.grisoft.com/.

## ERRATA: WINDOWS NT COMPARATIVE FEBRUARY 2004

The results were reviewed for two other products in the *Windows NT* comparative (*VB* February 2004, p.12), with the following outcome:

### *Alwil AVAST!*

After consultation with the developers a method was discovered by which the on-access function of *AVAST!* could be tested fully. The results of this re-testing were such that *Alwil*'s product gains a VB 100% award.


### *Sophos Anti-Virus*

*Sophos Anti-Virus* was noted in the *Windows NT* comparative as having missed one sample in the polymorphic test set. Further investigation determined that although this file was triply infected with W32/Zmist.D, the multiple infection had rendered the sample unable to replicate. Consequently this file has been removed from the test set. Although this does not affect percentages for other products, this does mean that *Sophos Anti-Virus* achieved 100% detection in the polymorphic test set, and indeed across all test sets.

# END NOTES & NEWS

**InterNetSecurity Trade Fair will be held 15–18 March 2004 in St Petersburg, Russian Federation**. For details see http://www.iegexpo.com/.

**InfoSec World Conference and Expo 2004 takes place 22–24 March 2004 in Orlando, FL, USA**. For details of the exhibition and a series of optional workshops see http://www.misti.com/.

**Infosecurity Europe 2004 will be held from 27–29 April 2004 in the Grand Hall Olympia, London, UK**. For all show details and registration enquiries see http://www.infosec.co.uk/.

**The 3rd Annual DallasCon Wireless Security Conference takes place 1–2 May 2004, in Dallas, TX, USA**. The conference will feature two tracks: one dedicated to the latest trends and threats in wireless security and a second focusing on general information security. For details see http://www.dallascon.com/.

**The EICAR Conference 2004 will be held in Luxembourg City, from 1–4 May 2004**. EICAR 2004 will feature only one stream, which will give in-depth coverage of issues including malware, critical infrastructure protection, legal and operational issues, and identity management and social issues. More information is available from http://www.eicar.org/.

**The 2004 World Computer and Internet Law Congress takes place on 6 and 7 May 2004 in Washington D.C., USA**. The event, presented by the Computer Law Association, will focus on providing practical advice on current IT law. For full details see http://www.cla.org/.

**The Black Hat Briefings and Training Europe takes place 17–20 May 2004 in Amsterdam, The Netherlands**. The call for papers for the Briefings closes on 25 March 2004. For more information see http://www.blackhat.com/.

**RSA Japan takes place 31 May to 1 June 2004 at the Akasaka Prince Hotel, Tokyo**. For details see http://www.rsaconference.com/.

**The Sixth Annual International Techno-Security Conference will be held 6–9 June 2004 in Myrtle Beach, CA, USA**. Topics will include computer forensics, Homeland security, intrusion detection, 'street smarts for cybercops', technical counter-terrorism, privacy issues, and security policies. For full details see http://www.technosecurity.com/.

**The 10th Annual Gartner IT Security Summit takes place 7–9 June 2004 in Washington, D.C., USA**. Topics include critical infrastructure protection, securing the workplace, security software and security strategies. See http://www3.gartner.com/.

**NetSec will take place 14–16 June 2004 in San Francisco, CA, USA.** The conference programme covers a broad array of topics, from the management issues of awareness, privacy and policy to more technical issues like wireless security, VPNs and Internet security. For full details see http://www.gocsi.com.

**MIS Training will host a CISO Executive Summit in Geneva on 16 and 17 June 2004**. This event for IT security leaders will cover the unique issues faced by CISOs. For more information contact Yvonne Hynes on +44 20 77798975 or email yhynes@misti.com.

**The 19th IFIP International Information Security Conference (SEC 2004) takes place 23–26 August 2004, in Toulouse, France**. Topics include intrusion detection, security architectures, security verification, multilateral security and computer forensics. A track will be dedicated to 'Security and Control of IT in Society'. For information see http://www.laas.fr/sec2004/ .

**The 14th Virus Bulletin International Conference and Exhibition, VB2004, takes place 29 September to 1 October 2004 at the Fairmont Chicago, IL, USA**. *Virus Bulletin* is seeking submissions from those wishing to present at the conference. Abstracts must be submitted by 31 March 2004. For more information about the conference, including the full call for papers, and details of sponsorship and exhibition opportunities, see http://www.virusbtn.com/.

**The 31st Annual Computer Security Conference and Expo will take place from 8–10 November 2004** at the Marriott Wardman Park in Washington, D.C., USA. More details will be available in due course from http://www.gocsi.com/.




## SUBSCRIPTION RATES

**Subscription price for 1 year (12 issues) including first-class/airmail delivery:** £195 (US$310)

**Editorial enquiries, subscription enquiries, orders and payments:**

Virus Bulletin Ltd, The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire OX14 3YP, England

Tel: +44 (0)1235 555139 Fax: +44 (0)1235 531889
Email: editorial@virusbtn.com www.virusbtn.com

# vb Spam supplement

CONTENTS



# NEWS & EVENTS

## CHINA SETS DEADLINE FOR SPAMMERS

The Internet Society of China's Anti-Spam Coordination Team (ASCT) has published a blacklist of mail servers sending spam. The list includes 626 IP addresses of mail servers sending spam inside and outside China: 62 in mainland China, 65 in Taiwan, 6 in Hong Kong and 493 outside China. If the servers have not stopped sending spam by 20 March 2004 the ASCT will take further steps 'to push them into anti-spam action'. Those that cease to send spam during this timeframe will be removed from the blacklist. This is the third edition of the ASCT's blacklist – the second edition, published in December 2003, included 27 IP addresses, of which 18 have now been removed. Full details can be found at http://www.isc.org.cn/.

## SMS SPAM GOES DOWN DOWN UNDER

Australia's Telecommunications Industry Ombudsman reports that a code of conduct aimed at preventing SMS spam has been highly effective – only 32 complaints about SMS spam have been filed over a three-month period. The anti-spam code, put together by the Australian Communications Industry Forum, is enforced by the Australian Communications Authority, which has the power to impose fines of up to AUD10 million on companies that fail to comply. While SMS spam is very different to the problem of unsolicited emails (since the sender must pay to send an SMS message), it seems that the threat of a hefty fine carries some weight.

## FINE FOR DIALLER SPAM

A UK watchdog has fined a US company for sending spam. The fine was imposed by the UK's regulatory body for the premium rate telecommunications industry, the ICSTIS (Independent Committee for the Supervision of Standards of Telephone Information Services) because the spam messages sent by *BW Telecom* contained peak rate porn dialler software (see *VB*, December 2002, p.12). The £75,000 fine was imposed after the ICSTIS received 240 complaints about the spam – in many cases users felt they had not been made sufficiently aware of what they were clicking on, and the dialler software failed to disconnect automatically once the cost of the call had reached the £20.00 limit set for premium rate services. As well as fining *BW Telecom* and barring access to the service for a year, the ICSTIS also ordered the company to reimburse those who were left out of pocket by its dialler scam.

## ISPs REFILE LAWSUITS

US Internet service providers *AOL* and *EarthLink* have each refiled lawsuits against prolific spammers.

A Florida man and married couple are accused by *AOL* of conspiring with two Americans based in Thailand to route mortgage scam solicitations to *AOL* customers and of developing a software program designed to circumvent *AOL*'s spam filters. Meanwhile, *EarthLink* has accused 16 individuals and companies in Florida, California, Tennessee and Michigan, of operating a spam ring, sending out more than 250 million emails advertising herbal supplements, Viagra and adult dating services.

Although both cases were originally filed in 2003, a federal court in Virginia ruled that *AOL* had shown insufficient evidence of damages caused by the defendants in Virginia. The company has refiled the case in Orlando. *EarthLink* has amended its original suit to include the names of the defendants.

## EVENTS

*101TechStrategies* will hold an Anti-Spam Summit from 17–19 March 2004 in San Francisco, USA. For details see http://www.101techstrategies.com/.

The First Conference on Email and Anti-Spam (CEAS) will be held 30 July to 1 August 2004 in Mountain View, CA, USA. Further details can be found at http://www.ceas.cc/.

# FEATURE

## THERE MUST BE 50 WAYS TO SAY 'VIAGRA'

*John Graham-Cumming*
Sophos Anti-Spam Task Force, USA

Since August 2002 I have been doing something that most people try to avoid on a daily basis: I read the spam that appears in my inbox. I read it not because I'm in search of a miracle weight-loss cure or cheap mortgage, but because I spend my time understanding the trickery spammers use to try to get through spam filters.

One of the words I see most often is 'Viagra', and because it's so common many simple spam filters treat it as a sure sign that a message is spam. Consequently, spammers spend their time trying to find new ways to warp the word enough to fool a spam filter and yet still be readable. You've probably seen some of these obfuscations in your inbox:

```
Vi@gra    V.i.a.g.r.a    V1agr@    Vìagrá
```

The list goes on and on. But you will not have seen many of the obfuscations used by spammers today: they are invisible to the human eye, but cause confusion for simple spam filters and, in a delicious piece of irony, make spam filtering easier for today's advanced spam filters.

I publish all the obfuscations that I have discovered on the web in the *Field Guide to Spam* (http://www.sophos.com/spaminfo/fieldguide/). Currently, there are 30 different tricks detailed with about two new ones appearing every month. In this article I shall introduce six spammers' tricks, each of which can be used to obscure the word Viagra.

Two of the tricks work on the plain text of an email message, but the others rely on HTML. Today, most email programs are able to understand emails that are sent using HTML, the language of the web.

HTML email enables people to send messages that include colours, different fonts and font sizes, and even pictures. HTML enables spammers to try to make their messages more enticing (who can resist 'Viagra' in large red letters?) and gives them a rich toolbox from which to create tricks to fool spam filters. It has become essential for any good spam filter to have at least a basic understanding of HTML.

### TRICK 1: LOST IN SPACE

Perhaps the simplest trick of all is to take a suspicious word like Viagra and insert a space after each letter:

```
V I A G R A
```

This fools simplistic spam filters that search for the word Viagra. Naturally, a more sophisticated spam filter can look for the pattern *<letter><space><letter><space>*... and reconstruct the suspicious word. For this reason, spammers use a variety of other characters to space out the word:

```
V'I'A'G'R'A    V*I*A*G*R*A
V.I.A.G.R.A    V-I-A-G-R-A
```

And the list could go on. Unfortunately for the spammer, it's pretty easy for a spam filter to look for these different patterns and figure out that the email is about Viagra. But this simple technique does raise a flag for anyone considering buying a spam filter: don't buy one that requires manual updating with the latest rules; get one with an automatic update service. Even staying current with this simple way of obscuring a word would require a large effort on your part.

Spammers, of course, test their spams against free and commercial anti-spam software and have obviously realised that this specific trick isn't working well, and so they have moved on to changing the actual letters of Viagra.

### TRICK 2: ZE FOREIGN ACCENT

A quick look at the ASCII table will reveal the presence of lots of accented vowels which spammers can use to obscure a suspicious word by swapping its vowels for their accented equivalents:

```
à á â ã ä å    ì í î ï      ù ú û ü
è é ê ë        ò ó ô õ ö
```

Just mixing and matching different accented 'a's and 'i's gives a spammer 144 different ways to write Viagra, such as:

```
Víagra    Viågra    Vîãgrä
```

English speakers ignore the accents and read the word, but a spam filter can be fooled. Of course, a spam filter programmed to recognise spammer trickery can map each accented vowel back to the basic letter to reconstruct the original word.

Since this trick and the previous one are easy pickings for today's spam filters, spammers have turned to HTML for more inventive ways to end up in your inbox.

### TRICK 3: A NUMBERS GAME

Another way to hide the word Viagra is to use a special feature of HTML designed for inserting special or non-English characters. These HTML entities are written starting with '&#' and ending with ';'. For example, to write the French accented character 'é' in HTML you write 'é', to write the Greek letter ∑ you write 'Ε'.

In fact all characters, including the standard English alphabet, have equivalent entities. The letter 'a', for example, can also be written 'a', and so a crafty spammer can rewrite the entire word 'Viagra' in entities:

```
&#86;&#105;&#97;&#103;&#114;&#97;
```

Once again, an up-to-date spam filter will understand HTML entities and make the conversion back to the real word. More sophisticated obfuscations of the word Viagra are possible by delving into HTML's formatting features.

## TRICK 4: HYPERTEXTUS INTERRUPTUS

HTML formatting information is specified using HTML tags: instructions written between < > brackets. For example, to specify that the word 'Hello' should appear in bold text you write: Hello. The  means 'start bold text', and the  means 'finish bold text'. The text between the two tags will appear bold when displayed using a web browser, or an email program that understands HTML.

Like most computer languages HTML also has a mechanism by which the creator of a page or message can insert a comment. These are there for other people to read, but are ignored when the HTML is displayed. A comment starts with '<!--' and ends with '-->'; anything written between the two is ignored by programs that display HTML.

Spammers use HTML comments to split up a suspicious word by inserting comments in the middle of the word. For example, Viagra can be broken up like this:

```
V<!--anon-->i<!--dinosaur-->a<!--hexagon-->g<!--
two-->r<!--mouse-->a
```

That odd-looking text will display as 'Viagra' in any email program that understands HTML. Many spam filters will be fooled by this technique because they don't understand HTML and are unable to see the word Viagra. Even worse, they might read the words in the comments and assume that the message is legitimate.

This is the most popular HTML trick used by spammers, and good spam filters now incorporate code that will strip out HTML comments before considering whether the message is spam or not. It's a simple task for a program to look for <!-- followed by --> and discard it.

In addition, a spam filter can consider the very presence of HTML comments to be suspicious.

## TRICK 5: THE BLACK HOLE

The incredible popularity of the previous trick has been its downfall: most spam filters now strip HTML comments. But splitting up words with bits of HTML remains a spammers' favourite. The Black Hole involves splitting up the suspicious word with spaces that have no width.

To specify the font size of a piece of text in HTML you write '<font size=X>', where X can be a value from 1 to 7 (7 being the largest size and 1 the smallest). For example, to say 'Hello' in the smallest font available you'd write:

```
<font size=1>Hello</font>
```

Programs like *Internet Explorer* and email programs *Outlook* and *Outlook Express* also accept the font size 0, i.e. the text has no size at all. So some spammers will put font size 0 together with a special piece of HTML syntax ' ', which is another way of writing the space character, to get a space with no width:

```
<font size=0> </font>
```

and then they use it to split the word Viagra up like this:

```
V<font size=0> </font>i<font
size=0> </font>a<font
size=0> </font>g<font
size=0> </font>r<font size=0> </font>a
```

The arms race between spammers and anti-spammers means that up-to-date spam filters need not only to understand HTML comments (see the previous trick), but also how HTML font sizes are specified. And once they do, spammers come up with even more devious tricks: if font size 0 is going to be spotted, how about font size 1?

## TRICK 6: THE MICRODOT

This recent innovation by spammers enables them to insert random letters in the middle of a word (thus making a spam filter that strips HTML read 'Viagra' as 'Vziagra', for example) and make those letters so tiny that they are almost invisible to the human eye. Welcome to the world of the microdot, or font size 1.

```
V<font size=1>z</font>iagra
```

Which when shown in an HTML-capable email program looks something like:

```
V.iagra
```

As you can see the letter z has been reduced to a tiny, almost invisible dot.

## SHOOTING THEMSELVES IN THE FOOT

With all the trickery that spammers deploy, you would be forgiven for thinking that spammers have the upper hand. In fact, the opposite is true. Good spam filters detect and catalogue the tricks used in a message and use that information to determine whether or not a message is spam. In fact, the most difficult messages to filter are those that are sent without any HTML and without any trickery. The more spammers resort to using trickery to try to obscure their messages, the easier those messages become to filter. [*A somewhat pleasing idea that spammers are hoist by their own petard - Ed.*]

# SUMMARY

## ASRG SUMMARY: FEBRUARY 2004

*Pete Sergeant*

Among the postings to the ASRG mailing list this month were a declaration that it's all over for challenge-response, a rather bleak view of the future and a lament about the lack of funding for law enforcement.

Yakov Shafranovich posted a link to a draft submitted to IETF entitled 'A no soliciting SMTP service extension', which would require senders to define their email with certain keywords. Philip Miller was not impressed, saying that work on consent frameworks was undertaken specifically to avoid 'content-specific solutions that are open to definition wars, redefinition, and even worse, cross-border legal wrangling'. He suggested that implementation of said standard would lead to the requirement that, in order to be compliant with every possible national law, senders check their mail against each and every registered keyword.

John Levine considered that the alternative would be for 'each country to make up its own rules', many of which would be contradictory. He pointed out that unsolicited commercial email (UCE) in Korea must start with the Korean word for advertisement, while the rules in the USA will require 'ADV' or similar: 'The same subject can't simultaneously be in Korean and English.'

Phillip Hallam-Baker decided 'it's all over for challenge-response', as apparently spammers are now setting up free 'adult' websites and asking visitors to the sites to 'solve' the non-machine-readable images that challenge-response systems use to verify that a human sent the originating message. However, it was pointed out that this would require spammers to provide a working return address to their spam – essentially dooming the scheme. There was some debate as to how cost-effective such a method would be for spammers, but no one had any specific figures.

In a later thread, Walter Dnes suggested that, in fact, it would only take one visually-impaired person with a good lawyer to get 'Turing test' schemes based on graphical recognition to become illegal anyway – this spawned a discussion on 'multi-modal' tests.

Walter also painted a rather dystopian future: 'There are "legitimate" spammers who do not want to see spamming made totally illegal, because they want to get in on the act once the "bad" spammers are shut down. The main difference between them is that "bad spammers" break the law, while "legitimate spammers" buy politicians to rewrite the law … If technical solutions do succeed in stopping spam, mark my word, you *will* see "must carry" legislation for "legitimate marketing email".'

A long thread kicked off on the subject of websites sending email on behalf of a visitor – such as the 'Email this article to a friend' feature offered by many online publications. It seems that some people believe that any email that you could not be absolutely certain came from a given sender was 'forged spam', and others didn't – however no particularly compelling solutions were suggested.

Yakov posted the Federal Trade Commission's (FTC) request for comments on its proposal to require those sending sexually-explicit UCE to label the email subject line with 'SEXUALLY-EXPLICIT-CONTENT', and to make this phrase the only thing a recipient would see when they first opened such an email. The deadline for feedback has passed, but you can read the original proposal at http://www.ftc.gov/opa/2004/01/adult.htm.

Fridrik Skulason requested a summary of 'RMX, DMP, SPF, LMAP, etc.', and was rewarded by Yakov's breakdown: 'The basic concept of LMAP is to publish in DNS a list of IPs that are authorized to use the domain name in the MAIL FROM or HELO arguments of the SMTP transaction. The technical differences between RMX, SPF and DMP [are] how this data is stored in DNS, how it is parsed, extensibility, and whether [the] HELO parameter is addressed.'

There was some discussion on the possibility of requiring originators to specify the size of their message at the SMTP level, so as to allow the throttling of connections from potential spammers, and so on. Peter Holzer was not convinced that size was a good indicator of the likelihood of a message being spam. He said: 'My users complain if they get a single 1k spam message per day and they complain if they don't get those 67 40MB *PowerPoint* presentations that someone sent them in an hour. There just isn't a correlation between number of messages, arrival rate, bandwidth, etc. and "spam".'

Yakov pointed out that the FTC had estimated that 70 per cent of spam is fraudulent and could be 'enforced' under existing laws. He lamented the fact that, while politicians are willing to talk about the problem, very few seem willing to give 'cold hard cash' to the enforcement agencies to allow them to do this.

Harry Tabak followed up with the insight that most spammers seem to be using zombies, and put forward the conclusion, based on his filtering attempts, that 'the cost to spammers of a failed delivery must be cheaper than the cost of pruning a mailing list' – zombie hosts with the same IP would keep trying to deliver to an email address that had rejected their emails before.